



ISO/IEC JTC 1/SC 27 **N2427**

ISO/IEC JTC 1/SC 27/WG 3 **N487**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN

DOC TYPE: Liaison Statement

TITLE: Liaison Statement to the Common Criteria Interpretations Management Board (CCIMB) in response to document SC 27 N 2390 (WG3 N483)

SOURCE: SC 27/WG 3 meeting, Columbia, MD, USA, October 1999

DATE: 1999-10-08

PROJECT: 1.27.16; 1.27.20; 1.27.21; 1.27.22;
Study period on Evaluation methodology

STATUS: In accordance with resolution 22 (SC 27 N 2466) of the 11th SC 27 plenary meeting in Columbia, USA, October 1999, this document has been sent to the CCIMB and is being circulated within SC 27 for information.

ACTION ID: FYI

DUE DATE:

DISTRIBUTION: P, O, L Members
W. Fumy, SC 27 Chairman
M. De Soete, T. Humphreys, M. Ohlin, WG-Conveners
U. van Essen, CCIMB Liaison Officer

MEDIUM: Server

NO. OF PAGES: 4

Secretariat ISO/IEC JTC 1/SC 27 –

DIN Deutsches Institut für Normung e. V., 10772 Berlin, Germany

Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: passia@ni.din.de

[HTTP://www.din.de/ni/sc27](http://www.din.de/ni/sc27)



ISO/IEC JTC 1/SC 27/WG 3 N487

ISO - International Organisation for Standardisation
IEC - International Electrotechnical Commission

JTC 1 - "Information Technology"
SC 27 - "Security Techniques"
WG 3 - "Security Evaluation Criteria"

TITLE: Liaison statement to the Common Criteria Interpretations Management Board

SOURCE: ISO/IEC JTC 1/SC 27/WG 3 Meeting, Columbia, October 1999

DATE: 1999-10-08

STATUS: For distribution to ISO/IEC JTC 1/SC 27

LIAISON STATEMENT

FROM: ISO/IEC JTC 1/SC 27/WG 3
TO: THE COMMON CRITERIA INTERPRETATIONS MANAGEMENT BOARD (CCIMB)

1. Expression of Thanks

ISO/IEC JTC 1/SC 27/WG 3 thanks the CCIMB Liaison Officer Ulrich van Essen for the report and presentation on the progress, status and plans for the CC project (ISO/IEC JTC 1/SC 27 N 2390, with the attached document "CC Maintenance Overview", CCIMB-99-039, available at <http://csrc.nist.gov/cc/t4/wg3>) and Lynne Ambuel for the comprehensive presentation on the Common Methodology for IT Security Evaluation (CEM).

2. Publication of IS 15408 and availability of IS 15408 on the Internet

The ballot on the Final Draft International Standard ISO/IEC ended on June 1st, 1999. 24 participating members (P-members) voted in favour of the standard, and there were no negative votes from participating or observing members (O-members). The vote was identical for all three parts. So IS 15408 was approved in this ballot. It is expected that the standard will be published in November. In addition the request from SC 27 to make IS 15408 freely available on the Web has been answered positively. IS 15408, all parts, will be made publicly available on the ITTF web site.

3. Production of CC version 2.1

ISO/IEC JTC 1/SC 27/WG 3 noted that a CC version 2.1 has been produced which reflects the changes made in the final phase of the standardisation process for IS 15408. It is appreciated that this development expresses the ongoing intent not to have any unnecessary divergence between IS 15408 and the Common Criteria.

4. Protection Profile Registration Authority

ISO/IEC JTC 1/SC 27/WG 3 is still discussing details of a Protection Profile registration process. The French National Standardisation Body AFNOR has expressed its willingness to act as such an authority. It is expected that registration will begin as soon as the International Standard 15292 is approved. According to the current ISO/IEC JTC 1/SC 27 programme of work the IS is expected to be published in 2001.

5. Definition and evaluation of packages in IS 15408 / CC version 2.1

The PP Registration Procedures is intended to provide for registration of packages of functional or assurance requirements, but it is not clear what constitutes a package or how to determine whether one is correct or complete. IS 15408-1 defines package as "a reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives." Via this definition, it is evident that the package can be viewed as a potential major sub-element of a PP or ST. However, although some guidance for package usage is contained in IS 15408-1 clause 4.4.2.1 and figure 4.7, the structure or required contents are not further defined, nor are explicit provisions made in IS 15408-3 for package evaluation. The notion of package usage or evaluation is not addressed in the Common Evaluation Methodology version 1.0. However, it is noted that certain families of class APE in IS 15408-3 appear applicable for package evaluation, in particular APE_REQ, APE_SRE and parts of APE_OBJ (i.e., 1.1D, 1.1C, 1.1E, 1.2E). WG 3 requests the CCIMB to provide further information on the anticipated content, structure, and evaluation of packages.

6. Criteria Maintenance

ISO/IEC JTC 1/SC 27/WG 3 noted the document "CC Maintenance Overview" which was distributed alongside the CCIMB Liaison Statement to ISO/IEC JTC 1/SC 27/WG 3 (ISO/IEC JTC 1/SC 27 N 2390). ISO/IEC JTC 1/SC 27/WG 3 understands that the CCIMB is prepared to deal with the necessary maintenance activities that arise through the application of the criteria. WG 3 encourages continued co-operation in this area.

7. WG 3 study period on evaluation methodology

ISO/IEC JTC 1/SC 27/WG 3 thanks the CC project for the technical contribution to the study period on evaluation methodology, "Common Methodology for Information Technology Security Evaluation (CEM), Part 2, version 1.0, August 1999", published at <http://csrc.nist.gov/cc>. The study period within ISO/IEC JTC 1/SC 27/WG 3 will continue through April 2000. It is planned that on the occasion of the WG 3 meeting in April 2000 a decision

concerning a New Work Item Proposal in the area of evaluation methodology will be made, which will include the aspect of whether the target of the work item will be an International Standard or a Technical Report.

8. Coverage of Common Evaluation Methodology and Mutual Recognition Arrangement

WG 3 understands that the CEMEB is currently setting priorities for its next period of work. It is noted that the CC Project's Mutual Recognition Arrangement, October 1998, contains the following wording in its Scope: "This Arrangement covers claims of compliance against any of the Common Criteria assurance components required for Evaluation Assurance Levels 1 through 4." It is also noted that the CEM Part 2 version 1.0 covers only EALs 1 through 4. WG 3 therefore acknowledges that completion of the items to support all of the current arrangement is of primary importance.

WG 3 takes note that augmentation beyond EAL4 level, along with international mutual recognition of certificates for products so evaluated, is strongly desired by commercial interests. In addition, several evaluation methodology principles have been identified as candidates for standardisation (see N494). In particular, WG 3 requests that the following be added to the list of priorities and submitted as contributions to the study period:

1. General guidance on applying the subjective terminology in IS 15408-3.
2. General guidance on determining the sufficiency of evaluator work.
3. General guidance on the application of IS 15408 to system evaluations.

In addition, highly critical and important commercial products, e.g. smart cards for financial applications and firewalls, require AVA_VLA components 3 and 4 to be appropriately secure. EAL4 (and therefore the CEM) contains methodology up to the vulnerability analysis component AVA_VLA.2. In the briefings provided on the CEM to WG 3 by CC Project members, it was identified that work on the CEM will continue in future, covering more assurance requirements in IS 15408. WG 3 requests that the CC Project give active consideration to placing a high priority on developing methodology for the higher AVA_VLA components and on incorporating recognition of evaluations including those components into the MRA.

9. Guide on the production of PPs and STs

A number of National Body comments on WD 15446 "Guide on the production of PPs and STs" were received, and as a consequence the document will undergo further revision. The updated draft of the Guide is due by November, 1999. According to the current ISO/IEC JTC 1/SC 27 programme of work the Technical Report is expected to be published in 2001.

10. Framework for IT security assurance

The ISO/IEC WD 15443 "Framework for IT security assurance" has reached a point where input from outside ISO/IEC JTC 1/SC 27/WG 3 is necessary in order to ensure that the overview on the various assurance methods is as complete as possible. Consequently ISO/IEC JTC 1/SC 27/WG 3 plans to inform several other bodies about the intent of the document, and ask for contributions. It is also requested that the CC project organisations contribute to the document by providing a description of the assurance methods they are currently applying or are otherwise involved in.